REMARKS

In response to the Office Action, Applicant requests reconsideration of the present application in view of the above claim amendments and the following remarks. The claim amendments simply add 4 dependent claims.

ARGUMENT

The Office Action includes claim rejections based on 35 U.S.C. §§ 102(e) and 103(a). Applicant respectfully traverses all of the rejections.

The Office Action also indicates that claims 3, 12, 15, 24, 27, 36, 39, and 48 would be allowable of rewritten in independent form to include the limitations of the respective base claims and any intervening claims.

The pending independent claims are claims 1, 13, 25, and 37.

35 U.S.C. § 102(e)

The Office Action rejects claims 1-2, 4-6, 10-11, 13-18, 22—23, 25-26, 28-30, 34-35, 37-39, 40-42, and 46-47 under 35 U.S.C. § 102(e) as being anticipated by U.S. patent no 6,327,652 to Paul England et al. ("England").

As explained in one or more previous responses, England pertains to a method for identifying the operating system running on a computer, based on "an identity associated with an initial component for the operating system, combined with identities of additional components that are loaded afterwards." In particular, after digital signatures for each component are validated, the operating system (referred to as a "digital rights management operating system" or "DRMOS") may assume a "trusted identity." (Abstract.) As far as it goes, England appears to describe reasonable aspects of a possible approach to supporting digital rights management.

The present application involves technology with embodiments that could also be applied in the arena of digital rights management. However, the present application, and in particular the pending claims, involve many features that

England does not disclose. For instance, claim 37 pertains to a system that includes a processor capable of operating in "an isolated execution mode in a ring 0 operating mode," where the processor also supports (a) one or more higher ring operating modes, as well as (b) "a normal execution mode in at least the ring 0 operating mode."

Accordingly, as explained in greater detail in the Detailed Description of the present application, a platform according one embodiment of the present invention may support privilege rings in the normal execution mode, as well as privilege rings in the isolated execution mode. (Figures 1A-1C and page 3, line 8, through page 10, line 27.)

In particular, claim 37 recites a processor that supports "an isolated execution mode in a ring 0 operating mode" and "a normal execution mode in ... the ring 0 operating mode."

For a valid rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (MPEP § 2131.01, quoting from Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)). Accordingly, the rejection of claim 37 is not proper unless England discloses a processor that supports "an isolated execution mode in a ring 0 operating mode" and "a normal execution mode in ... the ring 0 operating mode."

However, England makes absolutely no mention of "isolated execution mode," let alone "an isolated execution mode" and a "normal execution mode," each of which may operate in or include a "ring 0 operating mode." In fact, not one of the following terms appears anywhere in England: isolated execution, normal execution, privilege ring, ring 0, mode.

The Office Action asserts that England discloses a processor capable of operating in an isolated execution mode in a ring 0 operating mode, wherein the processor also supports (a) one or more higher ring operating modes, as well as (b) a normal execution mode in at least the ring 0 operating mode. Specifically, the Office Action asserts that England discloses those features at item 160 of Figure 1B, and at lines 44-59 of column 7. Applicant respectfully traverses those assertions.

In Figure 1B, item 160 is simply described as a "processor" within a central processing unit (CPU) 140. Lines 44-59 of column 7 go on to explain that CPU 140 may also include a "cryptographic accelerator 162," and that CPU 140 may perform "cryptographic functions, such as signing," with or without assistance from cryptographic accelerator 162. The cited lines also indicate that CPU 140 may be equipped with a unique pair of public and private keys, with the private key never to be revealed and to be used only for signing statements such as responses to challenges from a content provider. Figure 1B and lines 44-59 of column 7 say nothing about supporting normal and isolated execution modes in a ring 0 operating mode. For at least the foregoing reasons, the rejection of claim 37 is clearly improper.

Claims 1, 13, and 25 also involve a processor capable of operating in an isolated execution mode in a ring 0 operating mode, wherein the processor also supports (a) one or more higher ring operating modes, as well as (b) a normal execution mode in at least the ring 0 operating mode. With respect to claims 1, 13, and 25, the Office Action asserts that those features are disclose in England at item 801 of Figure 8, lines 45-61 of column 7, and lines 1-15 of column 17.

As discussed above, lines 45-61 of column 7 say nothing about supporting normal and isolated execution modes in a ring 0 operating mode. Figure 8 and lines 1-15 in column 17 simply explain that item 801 is an "OS storage key" that the CPU generates at the request of the DRMOS. None of the cited portions of England say anything about supporting normal and isolated execution modes in a ring 0 operating mode. For at least the foregoing reasons, the rejections of claim 1, 13, and 25 are also improper.

In addition, each independent claim also describes specific operations, such as encrypting a value or decrypting a value, to be performed "while operating in isolated execution mode." Since England says nothing about isolated execution mode, England can not possibly anticipate claims that recite encrypting a value or decrypting a value "while operating in isolated execution mode."

For at least the foregoing reasons, England does not anticipate any of the independent claims. Furthermore, since each dependent claim implicitly includes the features of its parent claim or claims, England does not anticipate any of the pending claims.

Furthermore, as explained in at least one previous response, the Detailed Description describes "isolated execution mode" as a mode of operation in which the platform allows access to a region of system memory that is protected by the platform hardware. Such regions of memory may be referred to as "isolated memory areas" or simply "isolated memory." The platform hardware prevents access to isolated memory when the system is not in isolated execution mode (e.g., when the system is in "normal execution mode").

Moreover, this response adds dependent claims (49-52) that explicitly refer to an isolated memory area that is accessible to the processor in the isolated execution mode but inaccessible in the normal execution mode. Since claim 49 depends from claim 37, claim 49 involves a processor that supports normal and isolated execution modes in a ring 0 operating mode, and a memory to include an isolated memory area that is inaccessible to the processor in the normal execution mode. Claims 50-52 involve the same or similar features. England does not disclose a processor to support normal and isolated execution modes in a ring 0 operating mode, and a memory to include an isolated memory area that is inaccessible to the processor in the normal execution mode. For at least the foregoing reasons, England does not anticipate claims 49-52.

35 U.S.C. § 103(a)

The Office Action rejects claims 7-8, 19-20, 31-32, and 43-44 under 35 U.S.C. § 103(a) as being unpatentable over England. Each of those claims depends from one of the independent claims discussed above. As indicated above, England does not disclose all of the features of the independent claims.

Furthermore, England does not suggest all of the features of the independent claims.

For instance, England does not disclose or suggest either encrypting a value or decrypting a value while operating in "isolated execution mode," as that term is explained in the independent claims. In fact, England does not disclose or suggest performing any kind of operations in isolated execution mode. England does not mention isolated execution mode at all. Consequently, England does not render any of the pending claims obvious.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims.

INFORMATION DISCLOSURE STATEMENTS

The Office Action requests that Applicant include a copy of the Information Disclosure Statement (IDS) that was submitted on December 16, 2003 with this response, so that the references could be consider by the Examiner. Copies of that IDS and the corresponding confirmation receipt are enclosed herewith.

Applicant respectfully requests confirmation that all references listed in that IDS have been considered.

CONCLUSION

In view of the foregoing, claims 1-8, 10-20, 22-32, 34-44, and 46-52 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927.

Prompt issuance of Notice of Allowance is respectfully requested.

-. Respectfully submitted,

Dated: October 10, 2005   / Michael R. Barre /

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450

On: October 10, 2005

Signature: Katherine Jennings